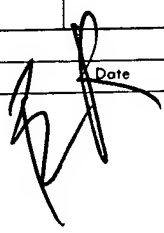


EXECUTIVE SECRETARIAT

ROUTING SLIP

TO:

		ACTION	INFO	DATE	INITIAL
1	DCI		X		
2	DDCI		X		
3	EXDIR		X		
4	D/ICS				
5	DDI				
6	DDA	X			
7	DDO				
8	DDS&T				
9	Chm/NIC				
10	GC				
11	IG				
12	Compt				
13	D/OLL				
14	D/PAO				
15	VC/NIC				
16	D/OS		X		
17	Ch/SECOM		X		
18					
19					
20					
21					
22					
SUSPENSE		 Date			

Remarks

DCI
EXEC

Executive Secretary

21 Oct 85

Date

3637 (10-81)

25X1

DIRECTOR OF CENTRAL INTELLIGENCE

25X1

19 October 1985

NOTE FOR: Director of Security

FROM: DCI

Jim:

The attached is for your information.



William J. Casey

Attachment:

Texas Business article,
dtd Oct 1985, "Worst-kept
Secrets" by William H. Inman



C-107

COVER STORY

Worst-kept secrets

Electronically, Texas companies are an open book, and the Russians are great readers.

by William H. Inman

It is the most damaging espionage case since Moscow obtained the secrets of America's H-bomb in the 1950s. Its implications ripple from the high-tech centers of California to the burgeoning Silicon Prairie of Texas.

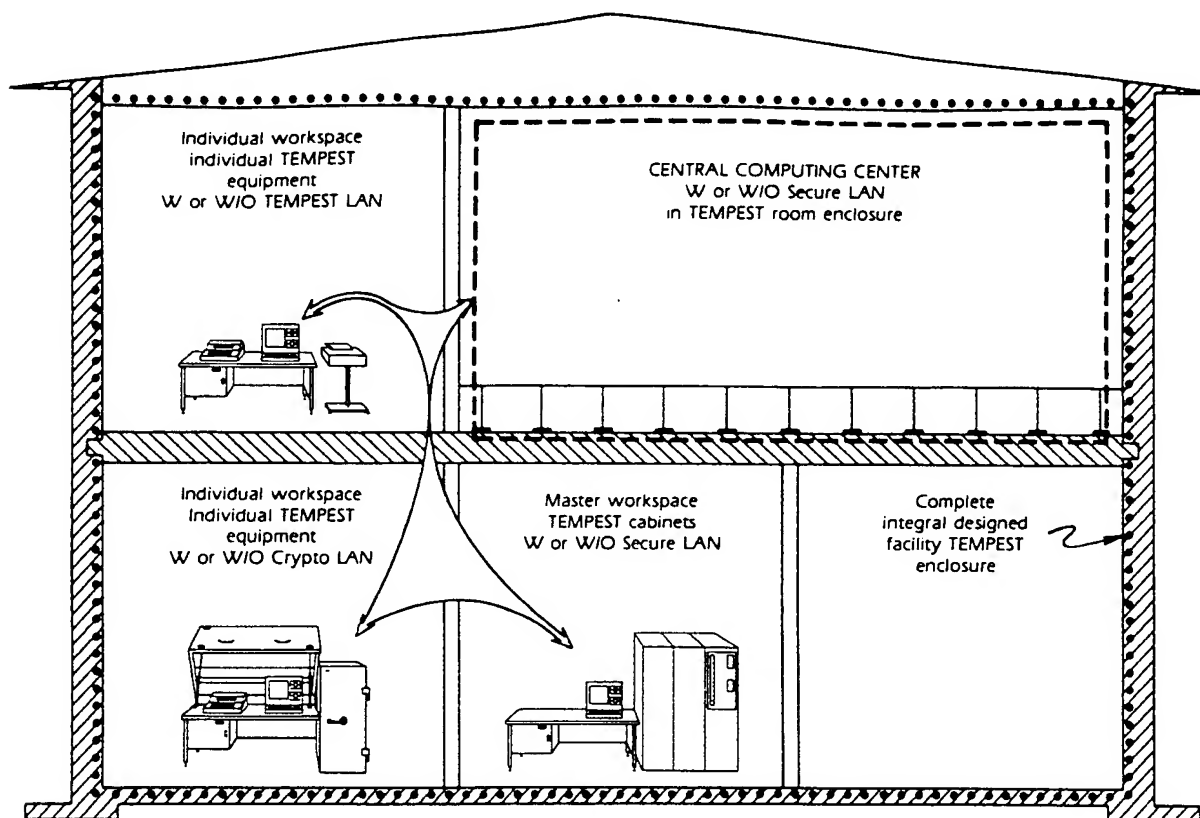
A tip from the former wife of John Anthony Walker set things in motion. When FBI agents eventually raided the home of Walker, who allegedly headed a family-based spy ring that sold secrets to the Soviets for over a decade, they confiscated a vast cache of secrets—including top Navy codes, blueprints for amphibious craft and drawings of heat-seeking missile circuitry. Three of the weapon plans, and details of their components, came from subcontractors in Texas. It is believed they were taken from "burn bags," classified material about to be incinerated on Navy ships, or by infiltrating the secret files at the businesses themselves. Nobody knows exactly how the spies obtained the documents. "We were surprised at the extent of the contraband," a Norfolk, Va., FBI investigator told TEXAS BUSINESS. "We have notified those (Texas) businesses that they must tighten up security."

For better or for worse, the state's new-found prosperity in microprocessors, computer research and computer-aided military hardware—Texas now ranks second behind only California in total volume of defense electronics research work—has introduced a new breed of observer to the state. He is the intelligence-gatherer, the

Dave Shannon

TEXAS BUSINESS 41

Cross section of typical TEMPEST security layers



expert in artificial intelligence who is acting to steal secrets on his own or as a proxy for some foreign power.

How real is the threat?

"We have absolutely no doubt there are Soviet agents in Texas," says a spokesman for one of the nation's private firms licensed in Texas by the National Security Agency to provide equipment secured against computer leaks. The company's specialty: providing anti-spy devices used in the rapidly developing and little-publicized field of TEMPEST. The name is not an acronym. It refers to the investigation and studies of compromising electronic emissions.

TEXAS BUSINESS interviewed various business executives and defense intelligence analysts, many of whom insisted on remaining unidentified, to sketch an outline of the hush-hush TEMPEST program and of the foreign threat it was designed to counter. "They (Soviet agents) are mixing well," says a source versed in artificial intelligence. "They're well trained. You do not see them on the street. They're very Americanized. The KGB (the Soviet es-

pionage branch) is very evident in Texas."

Intermediaries often used. When they do not act alone, they often are willing to hire American-born intermediaries, as the Walker case illustrates. "Many of those people have security clearances and they have access to all sorts of secret information," the source relates. "These are men willing to sell out their country for greed or because they are disgruntled with their job or because they want to make a philosophical point. They rationalize that they are not doing any real harm, but the facts speak for themselves."

Pentagon documents and published reports indicate the Soviets have installed a huge antenna in northwest Cuba geared to intercept electronic signals, especially telephone calls relayed by satellite across the southern United States. According to H. Ross Perot, chairman of Dallas's Electronic Data Systems Corp., roughly 2,000 to 3,000 Soviet agents roam the nation freely in search of America's high-technology secrets. "We know they come to Texas and are interested in Texas," says Perot.

Their presence is shadowy and subtle, in part because their signal-gathering equipment is so small and easily disguised. "It (the equipment) used to come in the form of a grocery van, something you would see delivering soda pop with a unique sort of TV antenna on top," reports one analyst. "Today's models are totally portable. They come in suitcase varieties. Honeywell makes them."

Because of the portability of these "suitcases," an enemy agent can slip undetected with all his equipment to a point near a secret testing facility or test zone, authorities say. Without appropriate precautions, the agent can sift the secrets he wants from the air—microwave emanations coming from a variety of sources, including electronic typewriters. Window panes provide an excellent medium for these wave transmissions. "A favorite," says one artificial intelligence expert, "is attaching sensitive equipment to water pipes. Water pipes greatly magnify vibrations."

And don't think the Soviets lack the ingenuity or initiative to use America's high-tech resources against her. Former

CIA director Stansfield Turner details in his book *Secrecy and Democracy* the gathering methods of Soviet consulates throughout the United States. Many of the diplomatic buildings bristle with arrays of antennae and, in some cases, are equipped to pick up the weak signals from typewriter keys. They planted just such typewriter receiving devices in the U.S. Embassy in Moscow recently. "The face of spying is, indeed, changing," Turner says. "We will have to adapt our countering techniques by placing more emphasis on uncovering technical systems that steal our secrets and by being more alert to detecting swashbuckling adventurers who spy for kicks."

That alertness begins at home; our phone conversations are not as private as we might think. Former CIA deputy director and NSA chief Bobby Inman attests that the Soviets are constantly monitoring our microwave telephone transmissions via satellite. "Americans simply do not realize the security breaches possible each time we pick up the telephone," says Inman, a retired Navy admiral who now heads Microelectronics and Computer Technology Corp.

A glossary of TEMPEST terms

BLACK DESIGNATION: A designation applied to wirelines, components, equipment and systems that handle only unclassified signals, and to areas in which classified signals occur.

COMPROMISE: Any occurrence that results in unauthorized persons' gaining access to classified or other information requiring protection.

COMPROMISING EMANATION: Unintentional data-related or intelligence-bearing signals which, if intercepted and analyzed, disclose the classified information transmitted.

EQUIPMENT RADIATION TEMPEST ZONE (ERTZ): A zone established as a result of determined or known TEMPEST equipment radiation characteristics. The zone includes all space within which a successful hostile intercept of compromising emanations is considered possible.

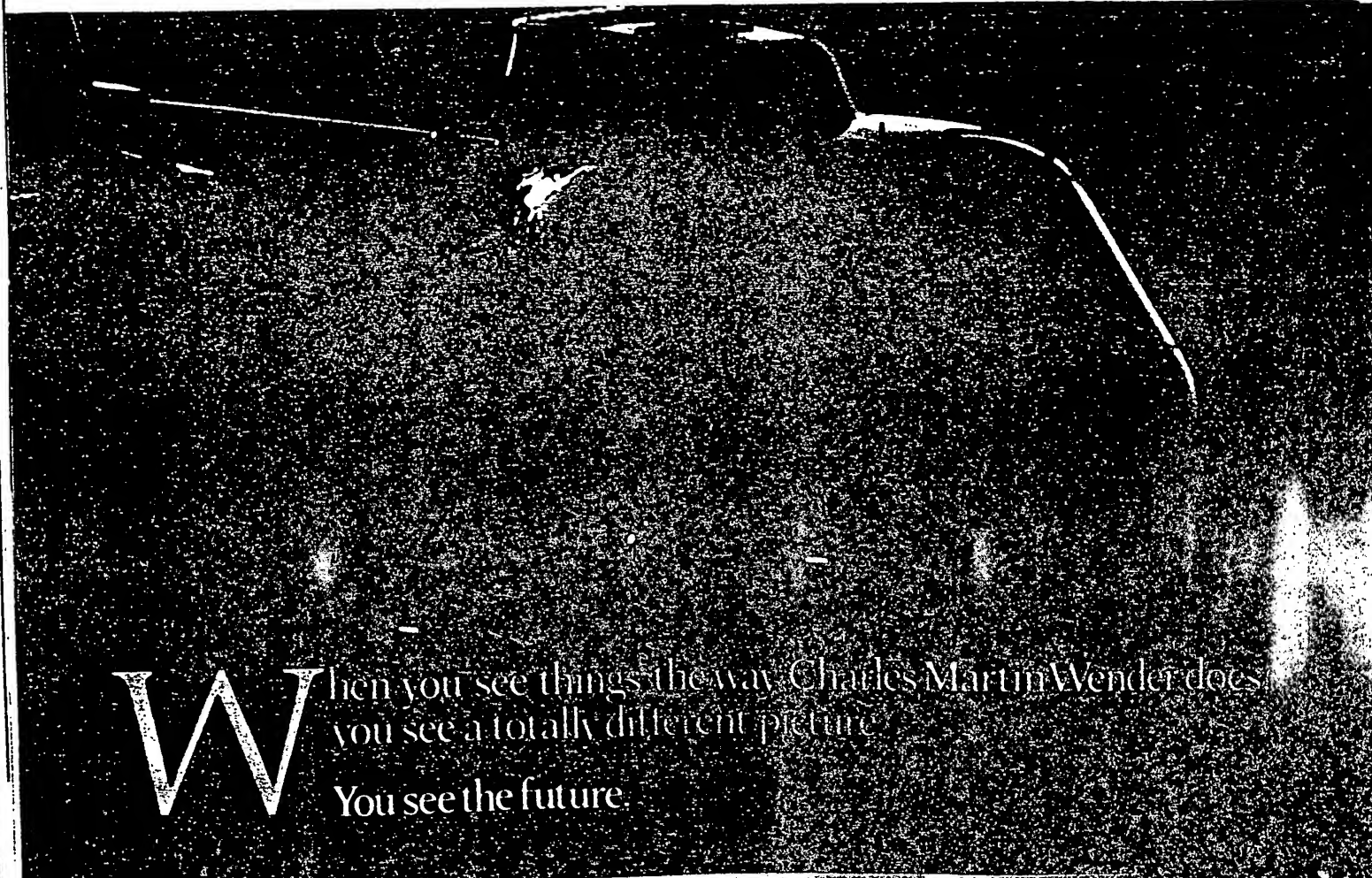
LIMITED EXCLUSION AREA: A room or enclosed area to which security controls have been applied to provide protection to information-processing system equipment.

ON-LINE CRYPTO-OPERATION: The use of crypto-equipment that is directly connected to a signal line, making encryption and transmission, or receptions and decryptions, or both together, a single continuous process.

TEMPEST: Name referring to investigations and studies of compromising emanations. It is sometimes used synonymously with the term compromising emanations, as in TEMPEST tests of TEMPEST inspections.

in Austin. NSA employees, in fact, have been told to minimize telephone communications. According to John Barron,

author of *KGB Today*, the Soviets monitor the calls of hundreds of thousands of Americans each day.



When you see things the way Charles Martin Wender does
you see a totally different picture.
You see the future.

Inter-company thievery. Foreign powers are not the only ones interested in stealing data. An electronics company seeking the secrets of a rival can turn to the many free-lance intelligence experts in the field for help. A law firm seeking to pull the rug from under a competitor in court in a million-dollar case or an employee of a bank seeking to embezzle funds through the hidden channels of a computer can draw upon a wide range of sophisticated techniques and private enterprise spies. Says one business analyst: "If you are in the habit of leaving classified data or important data on a disk in your computer overnight, then you could be a hit. Such data are retrievable unless properly encrypted. A gatherer can make a copy and go merrily on his—or her—way, nobody the wiser."

A team of professionals on the top floor of a bank building in Dallas or Houston or Austin could launch silent raids against a myriad of unsuspecting businesses. "You get on the right floor of the right building and aim a device called a spectrum analyzer at the window of your target," explains the analyst,

"and you zap everything you need in a very short time, and the company would never know it had been robbed." The devices come in a variety of forms, some as small as a man's umbrella.

But does Texas have the personnel who could pull off such a cunning assault? Indeed, it is training them every day. The Electronic Security Command in San Antonio, a military branch with the responsibility for plugging computer leaks throughout the region, employs a battery of highly competent electronic security sweepers, skilled in just such jobs. There is no evidence they have ever turned against their country or would in the future. But there is plenty of evidence that the technology and savvy are readily available. "The market is there," says one source. "There are very willing people who want the secrets. It's just a matter of latching onto the right people."

According to experts in the defense and electronics fields, a number of Texas industries are especially vulnerable to electronic infiltration. They include Varo Inc., LTV Corp., Texas Instruments, Rockwell International, General

Dynamics, Lockheed Missiles & Space, and E-Systems. This does not mean these companies do not have strong safeguards; they do. But it does indicate they work in areas of great interest to the Soviets and that their work areas are not completely secure. This is only a partial list, of course. There are far more industries vulnerable than are completely secure.

TEXAS BUSINESS, for example, followed up on a tip and sent a writer, without any credentials, into a classified zone at the Richardson, Tex., headquarters of TI. A side entrance door was not guarded, nor was it locked. "Oh yeah, that door needs to be fixed," an employee said later. Among other things, the company is at the forefront of the HARM missile project and a key supplier of the Army's night-vision equipment.

"There is a good-old-boy attitude in Texas that presupposes real espionage activity can't happen here," relates a TEMPEST products salesman. "That may have been true with the old Texas. But the Dallas/Fort Worth area and the corridor between San Antonio and

Seeking out and developing those areas of future growth and prosperity, Charles Martin Wender creates environments that are planned for tomorrow, not merely today. With instinct and foresight as his tools, he commands the attention of other developers and city planners who believe as he does. That long-range commitment and standard-setting excellence are essential to the San Antonio of the future.

Charles Martin Wender Real Estate and Investments • Commercial Office Building, Suite 1700 • 111 S. Alamo Street • San Antonio, Texas 78205

**CHARLES
MARTIN
WENDER**



Can your built-up roof take another winter?

Check your roof for blisters, cracks, splits and punctures. These are the problems that conventional roofs can develop after years of exposure to weather extremes. But the real problems occur when water leaks damage ceilings, walls, carpets, equipment, records and inventory.

Rugged Carlisle single-ply stands up to stress.

Today, there are over 13,000 warranted Sure-Seal™ roofs in service, with even the earliest installations still refusing to crack or leak after two decades of punishment by the sun, rain, wind, hail and snow.

Sure-Seal single-ply membrane, insulation and accessories can be installed right over top of your failing built-up roof—even in marginal weather—without interruptions to your business. And your new Carlisle roof is virtually maintenance-free, and can be warranted up to 15 years.

Now is the time to cover up with Carlisle single-ply.

We can deliver the materials and the technical expertise now—when you need them most. So call us, today.



Carlisle & Sure-Seal are trademarks of Carlisle Corporation.
©1983 Carlisle Corporation

Carlisle SynTec Systems
CARLISLE

THE DUNNE COMPANY, INC.
2741 SATSUMA
SUITE 107
DALLAS, TX 75229
(214) 241-7936

1217 WEST LOOP NORTH
SUITE 140
HOUSTON, TX 77055
(713) 956-1516

802 C BRANDI LANE
ROUND ROCK, TX 78664
(512) 244-6608

Eternal vigilance

The Soviets call it "part of the new wave of anti-Soviet hysteria in the United States," but American intelligence agents with the State Department's new Office of Foreign Missions are calling it smart.

The office, headed by former "head counterspy" at the FBI James E. Nolan, has tightened security controls across the country in an effort to keep under closer surveillance Soviet and other foreign diplomats in the U.S. Measures include such things as reciprocal treatment: Officials from another nation will be treated in this country in the same way American diplomats are treated in that particular foreign country. Though the restrictions apply to some U.S. allies, they are much stricter against so-called ideologic foes of the U.S., Eastern Bloc nations and, most specifically, the U.S.S.R.

The Office of Foreign Missions controls hotel accommodations, airline tickets, driver's licenses, car sales, prop-

erty rentals or sales, telephone installations, sales taxes, customs duties and other government fees and license plates. A new system using a letter code to designate certain closely watched countries has been instituted: DC for Cuba, FM for Libya, GQ for North Korea and SX for the Soviet Union.

In addition, Nolan's office oversees traffic routes by limiting areas in which foreign diplomats may travel. For instance, counties and cities in virtually every state in the nation have been designated off limits to Soviet officials. Sixteen of the proscribed counties are in Texas, including those of Harris, Dallas, Tarrant, Bexar and Travis (except Austin).

Nolan explains that the measures are designed to protect national security and sensitive facilities, and, he remarks, "You have to have that leverage or nobody is going to listen to you."

—Marion Buckley

Austin are full of businesses that the Soviets would love to learn more about. It's naive to think otherwise."

Varied vulnerability. What sort of equipment is vulnerable to infiltration? Just about any kind of electronic device which emits microwaves—everything from an ordinary pocket calculator to a full-size mainframe computer. Some of these devices need not be shielded, but with others, it makes little sense to leave them unprotected, especially considering the potential losses. Many of the losses that do occur are never reported to authorities.

In years past, TEMPEST was expensive. But the costs have dropped precipitously since NSA began issuing TEMPEST certificates to private industry. It once cost perhaps two to three times the price of an original IBM personal computer to protect it against intrusion. Today the cost is roughly half that amount. Prices vary from company to company, but here is a sampling: To retrofit an Apple II or Radio Shack TRS-80 Model III, it costs roughly \$4,990; a Pioneer video disk player, around \$9,450; a Xerox 610 electronic typewriter, about \$1,545, or around 25% above retail.

If the prices still seem a bit steep, con-

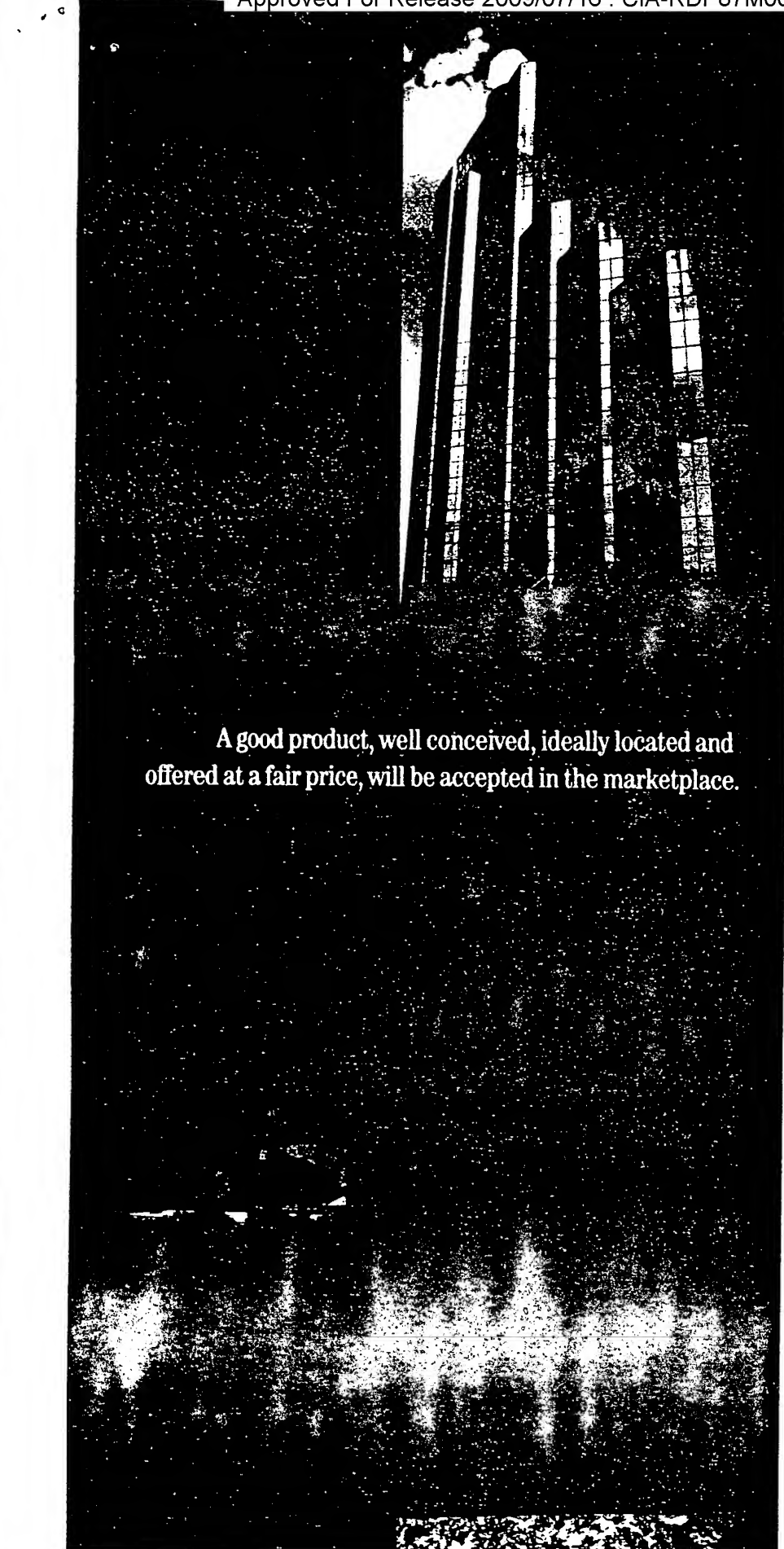
sider what must be done. Although specifics of the process remain classified for obvious reasons, here are the general methods:

- **Enclosure.** Surround all sides of the machine with metal plates, often copper or magnesium; a fine metal meshwork is often fitted over the viewing screen to reduce emissions.

- **Software alteration.** Get inside the machine to the microchip level and modify the signals they send to the rest of the system. This is obviously time-consuming and highly specialized.

- **Combination.** Combine the enclosure techniques with the software changes. All the modifications and shielding must pass government testing, and each configuration must be retested to be certified—a source of extra and hidden expense. One drawback of this totally secure system: The configuration cannot be expanded without thorough retesting.

Technology has taken this TEMPEST knowledge a step further. A company called Eye Identify Inc. now distributes a high-level identification system based on a unique human characteristic—the retinal eye pattern. A person peers into the EyeIdentification System 7.5 and the machine scans a circular area of the



A good product, well conceived, ideally located and offered at a fair price, will be accepted in the marketplace.

retina with a beam of ultra-low-density infrared light. The light reflected from the eye is picked up by a photo sensor and measured at 320 points along a 450-degree scan. The resulting wave form is then digitized and sent to a microprocessor, where it is stored. Since the retinal pattern is more distinctive than a person's fingerprint, the security system, if properly used, is considered nearly foolproof. None of the systems has yet been installed in Texas, but Rockwell and TI have purchased the units.

A la James Bond. Another James Bond-like device is the crypto-equipment, machines that scramble messages to prevent interception and interpretation. A crypto device can be installed in a computer modem to keep the telephone lines secure when transmitting data. A suitable unscrambler must be installed at the receiving end. An encryption device can even be installed within the computer disk, so that the data cannot be infiltrated when the disk is not being used.

Entire desk tops can be enclosed in armor-protected hoods, looking something like giant outdoor barbecue grills. Defense-minded businesses can purchase special engineering designs or hire specialized contractors who will protect whole floors in secured working areas. Many rooms are essentially metal-lined vaults and are laid out in such fashion that the most sensitive areas are protected by layers of wall and metal.

In 1983, Systematics General Corp., a leader in TEMPEST-enhanced products, began producing one of the more intriguing anti-spy products. It is called MicroFix and includes a TEMPEST-protected computer and nine specifically secured peripherals. The integrated computer system with telecommunications, data processing storage and retrieval capabilities has been used successfully by the Army for years for high-level battlefield intelligence gathering.

TEMPEST technology has grown rapidly in recent years, paralleling the need to protect increasingly sensitive equipment. As Herbert Shearin, executive manager for the TEMPEST project at the NSA, put it, "Tempest (was) once a low-profile concern (but) is now a very visible area of specialization in the government marketplace."

To understand the importance of TEMPEST is to understand the importance of keeping a secret. ☆